Rec'd PCT/PTO 07 FEB 2005
PCT/JP03/10186

日本国特許庁
JAPAN PATENT OFFICE

08.08.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

REC'D 26 SEP 2003
WIPO PCT

出願年月日
Date of Application: ２００２年　８月　８日

出願番号
Application Number: 特願２００２－２３１２８４

[ST. 10/C]: [ＪＰ２００２－２３１２８４]

出願人
Applicant(s): 松下電器産業株式会社

BEST AVAILABLE COPY

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００３年　９月１１日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０７４４９

【書類名】　特許願

【整理番号】　2037830120

【提出日】　平成14年 8月 8日

【あて先】　特許庁長官　　殿

【国際特許分類】　H04L 12/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　福岡　俊彦

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下システムテクノ株式会社内

【氏名】　和田　妙美

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100077931

【弁理士】

【氏名又は名称】　前田　　弘

【選任した代理人】

【識別番号】　100094134

【弁理士】

【氏名又は名称】　小山　　廣毅

【選任した代理人】

【識別番号】　100110939

【弁理士】

【氏名又は名称】　竹内　宏

【選任した代理人】
　【識別番号】　100110940
　【弁理士】
　【氏名又は名称】　嶋田　高久
【選任した代理人】
　【識別番号】　100113262
　【弁理士】
　【氏名又は名称】　竹内　祐二
【選任した代理人】
　【識別番号】　100115059
　【弁理士】
　【氏名又は名称】　今江　克実
【選任した代理人】
　【識別番号】　100115510
　【弁理士】
　【氏名又は名称】　手島　勝
【選任した代理人】
　【識別番号】　100115691
　【弁理士】
　【氏名又は名称】　藤田　篤史
【手数料の表示】
　【予納台帳番号】　014409
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0006010
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化復号化装置及び方法、暗号化装置及び方法、並びに復号化装置及び方法

【特許請求の範囲】

【請求項１】　暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報をＴＥＫ（traffic encryption key）制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記ＴＥＫ制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する暗号モード共用処理ブロックとを備え、

前記暗号モード共用処理ブロックは、

入力された鍵データを用いたＥＣＢ（electronic code book）処理を行うことによって、ＣＢＣ（cipher block chaining）モード及びＣＦＢ（cipher feedback）モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うものである

暗号化復号化装置。

【請求項２】　請求項１に記載の暗号化復号化装置において、

前記データ構造解析ブロックは、

前記ダウンストリームデータにおけるＭＰＥＧ（moving picture experts group）構造中のヘッダの解析を行い、前記ヘッダの情報に基づいて前記ＭＰＥＧ構造からＭＡＣ（media access control）構造を抜き出し、前記ＭＡＣ構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該ダウンストリームデータが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に

関する情報を前記ＴＥＫ制御用データとして出力するとともに、前記ＭＡＣ構造データから前記拡張ヘッダを除去して前記処理ブロック入力データとして出力するものである

ことを特徴とする暗号化復号化装置。

【請求項３】　請求項１に記載の暗号化復号化装置において、

前記データ制御ブロックは、

前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをＣＢＣモード、及びＣＦＢモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示す信号を前記モード選択信号として出力するものである

ことを特徴とする暗号化復号化装置。

【請求項４】　請求項１に記載の暗号化復号化装置において、

前記暗号モード共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、

前記処理ブロック入力データ、及び前記暗号処理データを入力とし、それぞれを遅延させて出力する遅延器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延器が出力する遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、

前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択して出

力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果として出力する第４のセレクタとを備え、

前記ＥＣＢ処理器は、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする暗号化復号化装置。

【請求項５】　請求項４に記載の暗号化復号化装置において、

前記ビットマスク器は、

前記モード選択信号が５６ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとして出力するものである

ことを特徴とする暗号化復号化装置。

【請求項６】　請求項４に記載の暗号化復号化装置において、

前記第１のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、その他の場合には、前記暗号処理データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

【請求項７】　請求項４に記載の暗号化復号化装置において、

前記第２のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処

理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

【請求項８】　請求項４に記載の暗号化復号化装置において、

前記第３のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処

理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択して出力するものである
ことを特徴とする暗号化復号化装置。

【請求項９】　請求項４に記載の暗号化復号化装置において、
前記第４のセレクタは、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記暗号処理データを選択して出力し、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、
前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合には、前記排他的論理和演算器の出力を選択して出力するものである
ことを特徴とする暗号化復号化装置。

【請求項１０】　請求項４に記載の暗号化復号化装置において、
前記ＥＣＢ処理器は、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合には、暗号化処理を行い、
前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、復号化処理を行い、
前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、暗号化処理を行うものである
ことを特徴とする暗号化復号化装置。

【請求項１１】　暗号化データを含むダウンストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報をＴＥＫ制御用データとして出力するとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

前記処理ブロック入力データに対して暗号化を行い、得られた暗号化結果を出力する暗号モード共用処理ブロックとを備え、

前記暗号モード共用処理ブロックは、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化を行うものである

暗号化装置。

【請求項１２】　請求項１１に記載の暗号化装置において、

前記暗号モード共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、

前記暗号処理データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、

前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果として出力する第４のセレクタとを備え、

前記ＥＣＢ処理器は、

前記ＥＣＢ処理として暗号化処理を前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする暗号化装置。

【請求項１３】　暗号化すべきデータを含むアップストリームデータを受け取り、そのデータ構造の解析を行って、ＴＥＫ制御用データを出力するとともに、前記暗号化すべきデータを前記処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

前記処理ブロック入力データに対して復号化を行い、得られた復号化結果を出力する暗号モード共用処理ブロックとを備え、

前記暗号モード共用処理ブロックは、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで復号化を行うものである

復号化装置。

【請求項１４】　請求項１３に記載の復号化装置において、

前記暗号モード共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記処理ブロック入力データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した処理ブロック入力データのうちのいずれかを選択して出力する第２のセレクタと、

前記暗号処理データと前記第２のセレクタの出力との排他的論理和を求めて、前記復号化結果として出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器とを備え、

前記ＥＣＢ処理器は、

前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする復号化装置。

【請求項１５】　暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータのデータ構造の解析を行って、暗号化に関する情報をＴＥＫ制御用データとして求めるとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして求めるデータ構造解析ステップと、

前記ＴＥＫ制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替えデータと、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データとを求めるデータ制御ステップと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替えデータに従って暗号化又は復号化を行って、暗号化結果又は復号化結果を求める暗号モード共用処理ステップとを備え、

前記暗号モード共用処理ステップは、

鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うものであり、前記モード選択データに示されたモードで暗号化又は復号化を行うものである

暗号化復号化方法。

【請求項１６】　請求項１５に記載の暗号化復号化方法において、

前記データ構造解析ステップは、

前記ダウンストリームデータにおけるＭＰＥＧ構造中のヘッダの解析を行い、前記ヘッダの情報に基づいて前記ＭＰＥＧ構造からＭＡＣ構造を抜き出し、前記ＭＡＣ構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該ダウンストリームデータが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に関する情報を前記ＴＥＫ制御用データとして出力するとともに、前記ＭＡＣ構造データから拡張ヘッダを除去して前記処理ブロック入力データとして求めるものである

ことを特徴とする暗号化復号化方法。

【請求項１７】　請求項１５に記載の暗号化復号化方法において、

前記データ制御ステップは、

前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをＣＢＣモード、及びＣＦＢモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示すデータを前記モード選択データとして求めるものである

ことを特徴とする暗号化復号化方法。

【請求項１８】　請求項１５に記載の暗号化復号化方法において、

前記暗号モード共用処理ステップは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとするＥＣＢ処理ステップと、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択する第１の選択ステップと、

前記処理ブロック入力データ、及び前記暗号処理データのそれぞれを遅延させる遅延ステップと、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延ステップで得られた遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択する第２の選択ステップと、

前記第１の選択ステップで選択されたデータと前記第２の選択ステップで選択されたデータとの排他的論理和を求める排他的論理和演算ステップと、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、前記排他的論理和、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択する第３の選択ステップと、

前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップと、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記暗号処理データ及び前記排他的論理和のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果とする第４の選択ステップとを備え、

前記ＥＣＢ処理ステップは、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを、前記モードに適合した鍵データを用いて前記第３の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである

ことを特徴とする暗号化復号化方法。

【請求項１９】　請求項１８に記載の暗号化復号化方法において、

前記ビットマスクステップは、

前記モード選択データが５６ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとするものである

ことを特徴とする暗号化復号化方法。

【請求項２０】　請求項１８に記載の暗号化復号化方法において、

前記第１の選択ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択し、その他の場合には、前記暗号処理データを選択するものである

ことを特徴とする暗号化復号化方法。

【請求項２１】　請求項１８に記載の暗号化復号化方法において、

前記第２の選択ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択し、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択するものである

ことを特徴とする暗号化復号化方法。

【請求項２２】　請求項１８に記載の暗号化復号化方法において、

前記第３の選択ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、前記排他的論理和を選択し、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択するものである

ことを特徴とする暗号化復号化方法。

【請求項２３】　請求項１８に記載の暗号化復号化方法において、

前記第４の選択ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、前記暗号処理データを選択し、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、前記排他的論理和を選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合には、前記排他的論理和を選択するものである

ことを特徴とする暗号化復号化方法。

【請求項２４】　請求項１８に記載の暗号化復号化方法において、

前記ＥＣＢ処理ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合には、暗号化処理を行い、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、復号化処理を行い、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、暗号化処理を行うものである

ことを特徴とする暗号化復号化方法。

【請求項２５】　暗号化データを含むダウンストリームデータのデータ構造の解析を行って、暗号化に関する情報をＴＥＫ制御用データとして求めるとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ステップと、

前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めるデータ制御ステップと、

前記処理ブロック入力データに対して暗号化を行って、暗号化結果を求める暗号モード共用処理ステップとを備え、

前記暗号モード共用処理ステップは、

鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができるものであり、前記モード選択データに示されたモードで暗号化を行うものである

暗号化方法。

【請求項２６】　請求項２５に記載の暗号化方法において、

前記暗号モード共用処理ステップは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとするＥＣＢ処理ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択する第１の選択ステップと、

前記暗号処理データを遅延させる遅延ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延ステップで得られた遅延した暗号処理データのうちのいずれかを選択する第２の選択ステップと、

前記第１の選択ステップで選択されたデータと前記第２の選択ステップで選択されたデータとの排他的論理和を求める排他的論理和演算ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、前記排他的論理和、及び前記遅延した暗号処理データのうちのいずれかを選択する第３の選択ステップと、

前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップと、

前記モード選択データに従って、前記暗号処理データ及び前記排他的論理和のうちのいずれかを選択して、前記暗号化結果とする第４の選択ステップとを備え、

前記ＥＣＢ処理ステップは、

前記ＥＣＢ処理として暗号化処理を前記モードに適合した鍵データを用いて前記第３の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである

ことを特徴とする暗号化方法。

【請求項２７】　暗号化すべきデータを含むアップストリームデータのデータ構造の解析を行って、ＴＥＫ制御用データとして求めるとともに、前記暗号化すべきデータを前記処理ブロック入力データとして求めるデータ構造解析ステップと、

前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めて出力するデータ制御ステップと、

前記処理ブロック入力データに対して復号化を行って、復号化結果を求める暗号モード共用処理ステップとを備え、

前記暗号モード共用処理ステップは、

鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるものであり、前記モード選択データに示されたモードで復号化を行うものである

復号化方法。

【請求項２８】　請求項２７に記載の復号化方法において、

前記暗号モード共用処理ステップは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとするＥＣＢ処理ステップと、

前記処理ブロック入力データを遅延させる遅延ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延ステップで得られた遅延した処理ブロック入力データのうちのいずれかを選択する第２の選択ステップと、

前記暗号処理データと前記第２の選択ステップで選択されたデータとの排他的論理和を求めて、前記復号化結果とする排他的論理和演算ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択する第３の選択ステップと、

前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップとを備え、

前記ＥＣＢ処理ステップは、

前記モード選択データに従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである

ことを特徴とする復号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号化及び暗号の復号化技術に関する。

【０００２】

【従来の技術】

デジタル双方向通信の代表的な例である双方向ＣＡＴＶ（cable television）システムでは、暗号化機能を実現するために、ＴＶ端末には暗号化機能が実装される。この暗号化機能としては、ＤＥＳ（data encryption standard）暗号に代表される秘密鍵暗号方式と、ＲＳＡ（Rivest-Shamir-Adleman）暗号に代表される公開鍵暗号方式とを組み合わせた方式が用いられる。

【０００３】

秘密鍵暗号方式とは、暗号化と復号化とに用いる鍵が共通であり、暗号化に用いられた鍵を用いて暗号化アルゴリズムを逆の順に実行することによって復号化を行い、暗号化を施す前の原文を得る方式である。この方式は、単純な排他的論理和の繰り返しアルゴリズムで実現されるもので、高速な処理を可能とする反面、送信側と受信側とで共通の鍵を保有する必要があり、鍵の配送・保持が困難であるという特徴を有する。

【０００４】

公開鍵暗号方式とは、落とし戸関数と呼ばれる、関数の演算は容易に実行でき、逆関数の演算を行うのは非常に困難であるような関数を利用するものであり、暗号化と復号化とに使用する鍵が異なるものである。したがって、鍵の配送・保持は容易に行える反面、秘密鍵暗号方式に比べて計算が複雑であり、秘密鍵暗号方式と比較して暗号化・復号化により多くの処理時間を要する。ただし、公開鍵暗号方式を使用して認証及び鍵配送を行い、秘密鍵暗号方式を使用してデータの暗号化を行うことによって、それぞれの利点を生かすことが可能となる。

【０００５】

さて、米国の標準方式であるＤＥＳ暗号方式では、ＥＣＢ（electronic code book）モードと呼ばれる、入力データサイズが６４ビット、出力データサイズが６４ビットの演算を基本処理として行う。この暗号方式の暗号化アルゴリズムに対して、あらかじめ文字又は単語が出現する頻度の分布を統計処理しておけば、入手した暗号化文の文字列パターンの頻度分布とのマッチングをとることにより、暗号化前の平文が推定されてしまう可能性がある。

【０００６】

そこで、暗号化された６４ビットの暗号ブロックと次に入力される６４ビットの入力データとの排他的論理和を演算して暗号文を作成する方法が考え出された。この方法を行って暗号化するモードをＣＢＣ（cipher block chaining）モードと呼んでいる。また、パケット通信のように通信を行う際のデータ単位があらかじめ決められている場合があるが、６４ビットを１ブロックとするブロック暗号化方式では、１ブロックのビット数（６４ビット）で割り切れないデータ単位が入力された場合には、１ブロックに満たない端数データができる。

【０００７】

データに端数部分がある場合には、１つ前のブロックの暗号解読演算結果と端数データの排他的論理和演算を実行し暗号化する。このような端数処理を行うモードの１つとして、ＣＦＢ（cipher feedback）モードがあり、ＣＦＢモードによって、データが６４ビットに満たない場合でも暗号文を得ることができる。

【０００８】

また、暗号化及び暗号解読（復号化）のいずれの演算においても、通常は５６ビットのデータを鍵として用いるが、特定の条件下では、４０ビットのデータを鍵として用いるモードも存在する。この場合、他のモードの場合と同様に、演算処理自体は６４ビット単位で行うが、鍵の有効データが４０ビットとなる。

【０００９】

このように、秘密鍵暗号方式演算においては複数のモード、すなわち、ＥＣＢモード、ＣＢＣモード及びＣＦＢモードのうちの１つと、５６ビット鍵モード又は４０ビット鍵モードのいずれかとの組み合わせに対応したモードが存在する。そして、デジタル双方向通信のセキュリティ機能を実現するために、すべてのモードに対応した暗号化装置又は復号化装置が一般的に用いられる。

【００１０】

【発明が解決しようとする課題】

従来のＤＥＳ暗号方式に基づく暗号化装置又は復号化装置は、複数のモードのそれぞれのための回路を備え、システムの要求に応じて複数のモードのいずれかを適宜選択し、そのモードのための回路を用いて暗号化演算又は暗号解読演算を行う構成となっている。

【００１１】

ところが、近年、暗号化又は暗号解読を必要とするシステムでは、単一の鍵のみを使用する場合は少なく、複数の鍵を使用して、それぞれの鍵に対応した演算を行う場合も増加してきている。

【００１２】

これを実現する装置は、各モードごとの暗号化又は暗号解読機能を備えた上、複数の鍵に対する演算を行う機能も必須となり、回路規模は莫大なものとなる。

一般的に、複数の鍵に対する演算は並列実行する必要があるため、処理が必要となる鍵の数が増大すると、装置としても、鍵の数に応じた数の処理回路を有する必要がある。

【００１３】

しかし、ＤＥＳの各モードは、ＥＣＢ処理と呼ばれる、ＤＥＳの基本処理を変形した処理が行われるものである。また、各モードを同時に並列実行する場合はほとんどない。このため、暗号化装置及び復号化装置において、複数のモードで処理回路を共用化して回路規模を削減することは可能である。

【００１４】

本発明は、複数のモードで処理回路を共用化することによって、回路規模を削減した暗号化復号化装置、暗号化装置、及び復号化装置を提供することを目的とする。

【００１５】

【課題を解決するための手段】

前記課題を解決するため、請求項１の発明が講じた手段は、暗号化復号化装置として、暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報をＴＥＫ（traffic encryption key）制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記ＴＥＫ制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する暗号モード共用処理ブロックとを備え、前記暗号モード共用処理ブロックは、入力された鍵データを用いたＥＣＢ（electronic code book）処理を行うことによって、ＣＢＣ（cipher block chaining）モード及びＣＦＢ（cipher feedback）モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示され

たモードで暗号化又は復号化を行うものである。

【００１６】

請求項１の発明によると、ＣＢＣモード又はＣＦＢモードのいずれのモードにおいても、同一のハードウェアによって暗号化及び復号化を行うことができる。したがって、暗号化復号化装置の回路規模を抑えることができる。

【００１７】

また、請求項２の発明では、請求項１に記載の暗号化復号化装置において、前記データ構造解析ブロックは、前記ダウンストリームデータにおけるＭＰＥＧ（moving picture experts group）構造中のヘッダの解析を行い、前記ヘッダの情報に基づいて前記ＭＰＥＧ構造からＭＡＣ（media access control）構造を抜き出し、前記ＭＡＣ構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該ダウンストリームデータが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に関する情報を前記ＴＥＫ制御用データとして出力するとともに、前記ＭＡＣ構造データから前記拡張ヘッダを除去して前記処理ブロック入力データとして出力するものである。

【００１８】

また、請求項３の発明では、請求項１に記載の暗号化復号化装置において、前記データ制御ブロックは、前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをＣＢＣモード、及びＣＦＢモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示す信号を前記モード選択信号として出力するものである。

【００１９】

また、請求項４の発明では、請求項１に記載の暗号化復号化装置において、前記暗号モード共用処理ブロックは、前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、前記処理ブロック入力データ、及び前記暗号処理データを入力とし、それぞれを遅延させて出力する遅延器と、前記暗号化／復号化切り替え信号及び前記モード選択信号に従

って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延器が出力する遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第３のセレクタと、前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果として出力する第４のセレクタとを備え、前記ＥＣＢ処理器は、前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである。

【００２０】

請求項４の発明によると、複数のモードにおいて暗号化及び復号化を行うことが、セレクタ等の簡単な回路を用いることによって実現できる。

【００２１】

また、請求項５の発明では、請求項４に記載の暗号化復号化装置において、前記ビットマスク器は、前記モード選択信号が５６ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとして出力するものである。

【００２２】

また、請求項６の発明では、請求項４に記載の暗号化復号化装置において、前記第１のセレクタは、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、その他の場合

には、前記暗号処理データを選択して出力するものである。

【００２３】

また、請求項７の発明では、請求項４に記載の暗号化復号化装置において、前記第２のセレクタは、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択して出力し、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力するものである。

【００２４】

また、請求項８の発明では、請求項４に記載の暗号化復号化装置において、前記第３のセレクタは、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択

信号がＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択して出力するものである。

【００２５】

また、請求項９の発明では、請求項４に記載の暗号化復号化装置において、前記第４のセレクタは、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記暗号処理データを選択して出力し、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合には、前記排他的論理和演算器の出力を選択して出力するものである。

【００２６】

また、請求項１０の発明では、請求項４に記載の暗号化復号化装置において、前記ＥＣＢ処理器は、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合には、暗号化処理を行い、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、復号化処理を行い、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、暗号化処理を行うものである。

【００２７】

また、請求項１１の発明は、暗号化装置として、暗号化データを含むダウンストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報をＴＥＫ制御用データとして出力するとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、前記処理ブロック入力デ

ータに対して暗号化を行い、得られた暗号化結果を出力する暗号モード共用処理ブロックとを備え、前記暗号モード共用処理ブロックは、入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化を行うものである。

【００２８】

請求項１１の発明によると、ＣＢＣモード又はＣＦＢモードのいずれのモードにおいても、同一のハードウェアによって暗号化を行うことができる。したがって、暗号化装置の回路規模を抑えることができる。

【００２９】

また、請求項１２の発明では、請求項１１に記載の暗号化装置において、前記暗号モード共用処理ブロックは、前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、前記暗号処理データを入力とし、これを遅延させて出力する遅延器と、前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第３のセレクタと、前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果として出力する第４のセレクタとを備え、前記ＥＣＢ処理器は、前記ＥＣＢ処理として暗号化処理を前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである。

【００３０】

請求項１２の発明によると、複数のモードにおいて暗号化を行うことが、セレクタ等の簡単な回路を用いることによって実現できる。

【００３１】

また、請求項１３の発明は、復号化装置として、暗号化すべきデータを含むアップストリームデータを受け取り、そのデータ構造の解析を行って、ＴＥＫ制御用データを出力するとともに、前記暗号化すべきデータを前記処理ブロック入力データとして出力するデータ構造解析ブロックと、前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、前記処理ブロック入力データに対して復号化を行い、得られた復号化結果を出力する暗号モード共用処理ブロックとを備え、前記暗号モード共用処理ブロックは、入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで復号化を行うものである。

【００３２】

請求項１３の発明によると、ＣＢＣモード又はＣＦＢモードのいずれのモードにおいても、同一のハードウェアによって復号化を行うことができる。したがって、復号化装置の回路規模を抑えることができる。

【００３３】

また、請求項１４の発明では、請求項１３に記載の復号化装置において、前記暗号モード共用処理ブロックは、前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、前記処理ブロック入力データを入力とし、これを遅延させて出力する遅延器と、前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した処理ブロック入力データのうちのいずれかを選択して出力する第２のセレクタと、前記暗号処理データと前記第２のセレクタの出力との排他的論理和を求めて、前記復号化結果として出力する排他的論理和演算器と、前記モード選択信号に従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力デ

ータのうちのいずれかを選択して出力する第３のセレクタと、前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器とを備え、前記ＥＣＢ処理器は、前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである。

【００３４】

請求項１４の発明によると、複数のモードにおいて復号化を行うことが、セレクタ等の簡単な回路を用いることによって実現できる。

【００３５】

また、請求項１５の発明は、暗号化復号化方法として、暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータのデータ構造の解析を行って、暗号化に関する情報をＴＥＫ制御用データとして求めるとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして求めるデータ構造解析ステップと、前記ＴＥＫ制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替えデータと、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データとを求めるデータ制御ステップと、前記処理ブロック入力データに対して前記暗号化／復号化切り替えデータに従って暗号化又は復号化を行って、暗号化結果又は復号化結果を求める暗号モード共用処理ステップとを備え、前記暗号モード共用処理ステップは、鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うものであり、前記モード選択データに示されたモードで暗号化又は復号化を行うものである。

【００３６】

また、請求項１６の発明では、請求項１５に記載の暗号化復号化方法において、前記データ構造解析ステップは、前記ダウンストリームデータにおけるＭＰＥＧ構造中のヘッダの解析を行い、前記ヘッダの情報に基づいて前記ＭＰＥＧ構造

からＭＡＣ構造を抜き出し、前記ＭＡＣ構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該ダウンストリームデータが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に関する情報を前記ＴＥＫ制御用データとして出力するとともに、前記ＭＡＣ構造データから拡張ヘッダを除去して前記処理ブロック入力データとして求めるものである。

【００３７】

また、請求項１７の発明では、請求項１５に記載の暗号化復号化方法において、前記データ制御ステップは、前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをＣＢＣモード、及びＣＦＢモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示すデータを前記モード選択データとして求めるものである。

【００３８】

また、請求項１８の発明では、請求項１５に記載の暗号化復号化方法において、前記暗号モード共用処理ステップは、前記ＥＣＢ処理を行い、得られた結果を暗号処理データとするＥＣＢ処理ステップと、前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択する第１の選択ステップと、前記処理ブロック入力データ、及び前記暗号処理データのそれぞれを遅延させる遅延ステップと、前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延ステップで得られた遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択する第２の選択ステップと、前記第１の選択ステップで選択されたデータと前記第２の選択ステップで選択されたデータとの排他的論理和を求める排他的論理和演算ステップと、前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、前記排他的論理和、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択する第３の選択ステップと、前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップと、前記暗号化／復号化切り替えデータ及

び前記モード選択データに従って、前記暗号処理データ及び前記排他的論理和のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果とする第４の選択ステップとを備え、前記ＥＣＢ処理ステップは、前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを、前記モードに適合した鍵データを用いて前記第３の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである。

【００３９】

また、請求項１９の発明では、請求項１８に記載の暗号化復号化方法において、前記ビットマスクステップは、前記モード選択データが５６ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとするものである。

【００４０】

また、請求項２０の発明では、請求項１８に記載の暗号化復号化方法において、前記第１の選択ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択し、その他の場合には、前記暗号処理データを選択するものである。

【００４１】

また、請求項２１の発明では、請求項１８に記載の暗号化復号化方法において、前記第２の選択ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択し、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデ

ータを、その後は前記遅延した処理ブロック入力データを選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択するものである。

【００４２】

また、請求項２２の発明では、請求項１８に記載の暗号化復号化方法において、前記第３の選択ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、前記排他的論理和を選択し、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択するものである。

【００４３】

また、請求項２３の発明では、請求項１８に記載の暗号化復号化方法において、前記第４の選択ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、前記暗号処理データを選択し、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、前記排他的論理和を選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合には、前記排他的論理和を選択するものである。

【００４４】

また、請求項２４の発明では、請求項１８に記載の暗号化復号化方法において、前記ＥＣＢ処理ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合には、暗号化処理を行い、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＢＣモードであることを示す場合には、復号化処理を行い、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがＣＦＢモードであることを示す場合には、暗号化処理を行うものである。

【００４５】

また、請求項２５の発明は、暗号化方法として、暗号化データを含むダウンストリームデータのデータ構造の解析を行って、暗号化に関する情報をＴＥＫ制御用データとして求めるとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ステップと、前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めるデータ制御ステップと、前記処理ブロック入力データに対して暗号化を行って、暗号化結果を求める暗号モード共用処理ステップとを備え、前記暗号モード共用処理ステップは、鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができるものであり、前記モード選択データに示されたモードで暗号化を行うものである。

【００４６】

また、請求項２６の発明では、請求項２５に記載の暗号化方法において、前記暗号モード共用処理ステップは、前記ＥＣＢ処理を行い、得られた結果を暗号処理データとするＥＣＢ処理ステップと、前記モード選択データに従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択する第１の選択ステップと、前記暗号処理データを遅延させる遅延ステップと、前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延ステップで得られた遅延した暗号処理データのうちのいずれかを選択する第２の選択ステップと、前記第１の選択ステップで選択されたデータと

前記第２の選択ステップで選択されたデータとの排他的論理和を求める排他的論理和演算ステップと、前記モード選択データに従って、前記処理ブロック入力データ、前記排他的論理和、及び前記遅延した暗号処理データのうちのいずれかを選択する第３の選択ステップと、前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップと、前記モード選択データに従って、前記暗号処理データ及び前記排他的論理和のうちのいずれかを選択して、前記暗号化結果とする第４の選択ステップとを備え、前記ＥＣＢ処理ステップは、前記ＥＣＢ処理として暗号化処理を前記モードに適合した鍵データを用いて前記第３の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである。

【００４７】

また、請求項２７の発明は、復号化方法として、暗号化すべきデータを含むアップストリームデータのデータ構造の解析を行って、ＴＥＫ制御用データとして求めるとともに、前記暗号化すべきデータを前記処理ブロック入力データとして求めるデータ構造解析ステップと、前記ＴＥＫ制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めて出力するデータ制御ステップと、前記処理ブロック入力データに対して復号化を行って、復号化結果を求める暗号モード共用処理ステップとを備え、前記暗号モード共用処理ステップは、鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるものであり、前記モード選択データに示されたモードで復号化を行うものである。

【００４８】

また、請求項２８の発明では、請求項２７に記載の復号化方法において、前記暗号モード共用処理ステップは、前記ＥＣＢ処理を行い、得られた結果を暗号処理データとするＥＣＢ処理ステップと、前記処理ブロック入力データを遅延させる遅延ステップと、前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延ステップで得られた遅延した処理ブロ

ック入力データのうちのいずれかを選択する第２の選択ステップと、前記暗号処理データと前記第２の選択ステップで選択されたデータとの排他的論理和を求めて、前記復号化結果とする排他的論理和演算ステップと、前記モード選択データに従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択する第３の選択ステップと、前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップとを備え、前記ＥＣＢ処理ステップは、前記モード選択データに従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである。

【００４９】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら説明する。

【００５０】

図１は、本発明の実施形態に係る暗号化復号化装置の構成を示すブロック図である。図１の暗号化復号化装置は、データ構造解析ブロック２と、暗号モード共用処理ブロック４と、データ制御ブロック６とを備えている。図１の暗号化復号化装置は、例えば、センター装置及び複数の端末装置により構成される双方向通信網において、端末装置の１つを構成するものである。センター装置は、暗号化されたデータを含むダウンストリームデータＳＤを端末装置に送信する。ダウンストリームデータＳＤには、映像データ及び伝送制御データが含まれている。一方、端末装置は、暗号化すべきデータを含むアップストリームデータを受け取り、暗号化してセンター装置に対して送信する。

【００５１】

データ構造解析ブロック２は、ダウンストリームデータＳＤを受け取り、その構文解析を行う。ダウンストリームデータＳＤは、例えば、映像データにおけるＭＰＥＧ構造と、ＭＰＥＧ構造に埋め込まれているネットワーク処理用のサブレイヤであるＭＡＣ（media access control）構造を有している。

【００５２】

まず、データ構造解析ブロック２は、ＭＰＥＧ構造データ中のヘッダ部分を解析し、ＭＡＣ構造データを抜き出すための情報を抽出した後に、ＭＡＣ構造データを抜き出す。次に、ＭＡＣ構造データ中のヘッダ部分を解析し、通常のヘッダのみでなく、拡張ヘッダと呼ばれる拡張されたフィールドが存在する場合は、この拡張ヘッダを解析する。拡張ヘッダは、データ構成の拡張を可能にするものであって、暗号化の有無、その他の暗号化又は復号化のための処理に必要となる情報を有している。

【００５３】

拡張ヘッダが存在しない場合、データ構造解析ブロック２は、ダウンストリームデータＳＤが暗号化されていないと判断する。この場合、データ構造解析ブロック２は、ＴＥＫ制御用データＴＫを例えば値“０”に固定し、データ制御ブロック６に出力する。

【００５４】

拡張ヘッダが存在する場合、データ構造解析ブロック２は、暗号化に関する情報を格納するフィールドを解析する。暗号化されていないことを確認した場合には、拡張ヘッダが存在しない場合と同様の処理を行う。暗号化されていることを確認した場合には、暗号化に関する情報であるＳＩＤ（service ID）及びキーシーケンスナンバー（key sequence number）を拡張ヘッダから抽出し、ＴＥＫ制御用データＴＫとしてデータ制御ブロック６に出力する。

【００５５】

また、データ構造解析ブロック２は、暗号化すべきデータをアップストリームデータＳＵとして受け取り、その構文解析を行う。データ構造解析ブロック２は、アップストリームデータＳＵに含まれるデータからＳＩＤ及びキーシーケンスナンバーを抽出し、ＴＥＫ制御用データＴＫとしてデータ制御ブロック６に出力する。

【００５６】

データ構造解析ブロック２は、ダウンストリームデータＳＤに含まれるＭＰＥＧ構造を有する暗号化データ、又はアップストリームデータＳＵに含まれる暗号

化すべきデータを、処理ブロック入力データＥＣとして暗号モード共用処理ブロック４に出力する。

【００５７】

データ構造解析ブロック２は、受信したダウンストリームデータＳＤ又はアップストリームデータＳＵのパケットのビット数をカウントし、ストリームのパケットのビット数が６４ビット以下、６４ビットの倍数、又は６４ビットの倍数と６４ビット以下の端数との和のいずれであるか、及びパケットのうち処理ブロック入力データＥＣとして出力したビット数（パケットカウント）を求める。データ構造解析ブロック２は、求められた結果、並びに、ダウンストリームデータＳＤを受け取った場合には復号化すべきであることを、及びアップストリームデータＳＵを受け取った場合には暗号化すべきであることをもＴＥＫ制御用データＴＫとしてデータ制御ブロック６に出力する。

【００５８】

次に、データ制御ブロック６は、データ構造解析ブロック２から受信したＴＥＫ制御用データＴＫを用いて処理を行う。まず、ＳＩＤ及びキーシーケンスナンバーをチェックして、これらのデータがあらかじめ決められている有効な数値であるかどうかを判断する。無効な数値であると判断した場合は、何も処理を行わない。有効な数値であると判断した場合は、データ制御ブロック６は、５６ビット鍵モードであるか否かをチェックする。暗号化及び復号化には、５６ビットの鍵が標準として用いられるが、これ以外の長さの鍵も用いられる。以下では例として、５６ビット又は４０ビットの鍵が用いられるものとする。５６ビット鍵モードであるか否かは、ＳＩＤ及びキーシーケンスナンバーに一意に対応する。データ制御ブロック６は、５６ビット鍵モードであるか否かを示す情報をモード選択信号ＭＳとして出力する。

【００５９】

データ制御ブロック６は、ＴＥＫ制御用データＴＫに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号ＳＳを暗号モード共用処理ブロック４に出力する。また、データ制御ブロック６は、ＴＥＫ制御用データＴＫを参照して、処理ブロック入力データＥＣのパケットのビット数が６４

ビット以下の場合はＣＦＢモードを示す信号を、６４ビットの倍数である場合はＣＢＣモードを示す信号を、モード選択信号ＭＳとして暗号モード共用処理ブロック４に出力する。

【００６０】

パケットのビット数が６４ビットの倍数と６４ビット以下の端数との和である場合は、データ制御ブロック６は、パケットカウントに応じて、モード選択信号ＭＳを次のように切り替える。すなわち、データ構造解析ブロック２が６４ビットの倍数に相当する処理ブロック入力データＥＣを出力しているときは、ＣＢＣモードを示す信号を、６４ビット以下の端数に相当する処理ブロック入力データＥＣを出力しているときは、ＣＦＢモードを示す信号を、データ制御ブロック６がモード選択信号ＭＳとして出力する。また、データ制御ブロック６は、それぞれのモードの処理を開始する初期状態、又はその後の定常状態のいずれであるかも、モード選択信号ＭＳとして出力する。

【００６１】

また、データ構造解析ブロック２は、受信したダウンストリームデータＳＤ又はアップストリームデータＳＵに応じて、ＥＣＢモードで処理すべきか否かをＴＥＫ制御用データＴＫによってデータ制御ブロック６に通知する。ＥＣＢモードで処理すべき場合には、データ制御ブロック６は、ＥＣＢモードを示す信号をモード選択信号ＭＳとして出力する。

【００６２】

このように、データ制御ブロック６は、ＳＩＤ、キーシーケンスナンバー、及びパケットカウント等に応じてモード選択信号ＭＳを切り替えて、暗号モード共用処理ブロック４に出力する。

【００６３】

暗号モード共用処理ブロック４は、外部から入力された初期ベクタデータＩＶ、及び鍵データＫＤを用いたＥＣＢ処理を行うことによって、ＥＣＢモード、ＣＢＣモード及びＣＦＢモードのいずれにおいても、処理ブロック入力データＥＣに対して暗号化及び復号化を行うことができるように構成されている。暗号モード共用処理ブロック４は、モード選択信号ＭＳに示されたモードで、暗号化／復

号化切り替え信号ＳＳに従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を処理済データＤＣとして出力する。

【００６４】

図２は、図１の暗号モード共用処理ブロック４の構成の例を示すブロック図である。図２の暗号モード共用処理ブロック４は、第１のセレクタ４１と、第２のセレクタ４２と、第３のセレクタ４３と、第４のセレクタ４４と、ビットマスク器４６と、ＥＣＢ処理器４７と、遅延器４８と、排他的論理和演算器４９とを備えている。

【００６５】

第１のセレクタ４１は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号ＭＳに従って、処理ブロック入力データＥＣ、及びＥＣＢ処理器４７が出力する暗号処理データＰＤのうちのいずれかを選択して排他的論理和演算器４９に出力する。

【００６６】

遅延器４８は、処理ブロック入力データＥＣ、及び暗号処理データＰＤを入力とし、それぞれを、ＥＣＢ処理器４７が６４ビットのデータに対してＥＣＢ処理を行うのに要する時間だけ遅延させて、第２のセレクタ４２に出力する。

【００６７】

第２のセレクタ４２は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号ＭＳに従って、処理ブロック入力データＥＣ、初期ベクタデータＩＶ、並びに、遅延器４８が出力する遅延した処理ブロック入力データＥＣＤ及び遅延した暗号処理データＰＤＤのうちのいずれかを選択して排他的論理和演算器４９に出力する。

【００６８】

排他的論理和演算器４９は、第１のセレクタ４１の出力と第２のセレクタ４２の出力との排他的論理和を対応するビット毎に求めて第４のセレクタ４４に出力する。

【００６９】

第３のセレクタ４３は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号

ＭＳに従って、処理ブロック入力データＥＣ、排他的論理和演算器４９が出力する排他的論理和データＥＲ、遅延した処理ブロック入力データＥＣＤ、及び遅延した暗号処理データＰＤＤのうちのいずれかを選択してＥＣＢ処理器４７に出力する。

【００７０】

ビットマスク器４６は、鍵データＫＤを、モード選択信号ＭＳに従って必要に応じてその一部をマスクして、モードに適合した鍵データとしてＥＣＢ処理器４７に出力する。

【００７１】

第４のセレクタ４４は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号ＭＳに従って、暗号処理データＰＤ及び排他的論理和演算器４９が出力する排他的論理和データＥＲのうちのいずれかを選択して、暗号化結果又は復号化結果として出力する。

【００７２】

ＥＣＢ処理器４７は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号ＭＳに従って、ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを、第３のセレクタ４３の出力に対して行う。ＥＣＢ処理器４７は、ビットマスク器４６が出力するモードに適合した鍵データを用いてＥＣＢ処理を行い、得られた結果を暗号処理データＰＤとして第１のセレクタ４１、第４のセレクタ４４、及び遅延器４８に出力する。

【００７３】

図３は、図１の暗号モード共用処理ブロック４が行う処理の流れを示す説明図である。図３において、上段は暗号化処理の流れを示し、下段は復号化処理の流れを示している。処理Ｅ１，Ｅ２，Ｅ３，Ｅ９，Ｄ１，Ｄ２，Ｄ３，Ｄ９はそれぞれＥＣＢ処理を表している。暗号モード共用処理ブロック４は、暗号化処理及び復号化処理のいずれの場合にも、ＣＢＣモードによる処理を行う必要があるときは、ＣＢＣモードによる処理を連続して行い、その後、必要に応じてＣＦＢモードによる処理を行う。

【００７４】

図３では、処理Ｅ９，Ｄ９を含む最も右の列の処理はＣＦＢモードの処理を示している。処理Ｅ１，Ｅ２，Ｅ３，Ｄ１，Ｄ２，Ｄ３を含むその他の３つの列の処理はＣＢＣモードの処理を示している。また、「ＩＶ」は初期ベクタデータ、「Ｄ」は暗号化されていないデータ、「Ｉ」は、図３上段の暗号化処理の場合はＥＣＢ処理前、下段の復号化処理の場合はＥＣＢ処理後のデータを示す。また、「Ｃ」は暗号化データ、「Ｅｎｃｒｙｐｔ」はＥＣＢ処理器４７におけるＥＣＢ処理が暗号化処理であること、「Ｄｅｃｒｙｐｔ」はＥＣＢ処理器４７におけるＥＣＢ処理が復号化処理であることを示す。実際のＥＣＢ処理には鍵データを用いるが、図３においては、鍵データのデータフローは省略している。図３の処理の流れは、５６ビット鍵モードであるか否かにかかわらず同様である。

【００７５】

図４は、図１の暗号モード共用処理ブロック４の第１～第４のセレクタ４１～４４が選択するデータの組み合わせを示す説明図である。暗号モード共用処理ブロック４の復号化処理時の動作について、図２、図３の下段、及び図４を参照して説明する。この場合、暗号モード共用処理ブロック４には、暗号化／復号化切り替え信号ＳＳとして、復号化を示す信号が入力される。５６ビット鍵モードであるか否か、ＣＢＣモード及びＣＦＢモードのうちのいずれであるか、初期状態及び定常状態のうちのいずれであるかによって場合を分けて説明する。ＥＣＢ処理器４７におけるＥＣＢ処理は、ＣＢＣモードの場合は復号化処理、ＣＦＢモードの場合は暗号化処理である。

【００７６】

１）５６ビット鍵モードであり、かつ、ＣＢＣモードの初期状態である場合（図４のＤＥＣ－ＣＢＣ　Ｉｎｉｔの場合）

この場合は、図３の下段の処理Ｄ１及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック４は、暗号化データＣを入力とし、ＥＣＢ処理として「Ｄｅｃｒｙｐｔ」処理を行って、データＩを求める。暗号モード共用処理ブロック４は、求められたデータＩと入力された初期ベクタデータＩＶとの排他的論理和を求めて、暗号化されていないデータＤとして出力する。

【００７７】

この場合の処理を、図２を参照して説明する。暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＢＣモードの初期状態であることを示す信号が入力される。

【００７８】

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、初期ベクタデータＩＶを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと初期ベクタデータＩＶとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

【００７９】

第３のセレクタ４３は、処理ブロック入力データＥＣを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

【００８０】

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された処理ブロック入力データＥＣに対してＥＣＢ処理として復号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして復号化結果を出力する。

【００８１】

２）５６ビット鍵モードであり、かつ、ＣＢＣモードの定常状態である場合（図４のＤＥＣ－ＣＢＣ　Ｎｏｒｍａｌの場合）

この場合は、図３の下段の処理Ｄ２又はＤ３及びこれらのそれぞれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック４は、暗号化データＣを入力とし、「Ｄｅｃｒｙｐｔ」処理を行って、データＩを求める。暗号モード共用処理ブロック４は、求められたデータＩとその前のＥＣＢ処理で用いた暗号化データＣとの排他的論理和を求めて、暗号化されていないデータＤとして出力する。

【００８２】

この場合の処理を、図２を参照して説明する。暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＢＣモードの定常状態であることを示す信号が入力される。

【００８３】

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、遅延器４８が出力する遅延された処理ブロック入力データＥＣＤを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと遅延された処理ブロック入力データＥＣＤとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

【００８４】

第３のセレクタ４３は、処理ブロック入力データＥＣを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

【００８５】

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された処理ブロック入力データＥＣに対してＥＣＢ処理として復号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして復号化結果を出力する。

【００８６】

３）５６ビット鍵モードではなく、かつ、ＣＢＣモードの初期状態である場合

４）５６ビット鍵モードではなく、かつ、ＣＢＣモードの定常状態である場合

これらの場合は、それぞれ１），２）の場合と次の点を除いて同じである。すなわち、暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードではないことを示す信号が入力される。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードではないことを示す信号が入力されているので、入力された５６ビットの鍵データＫＤのうち、必要がないビット

（例えば上位１６ビット）をマスクして、４０ビット鍵データとしてＥＣＢ処理器４７に出力する。ＥＣＢ処理器４７は、ビットマスク器４６から出力された４０ビット鍵データを用いてＥＣＢ処理を行う。

【００８７】

５）５６ビット鍵モードであり、かつ、ＣＦＢモードの初期状態である場合（図４のＤＥＣ－ＣＦＢ　Ｉｎｉｔの場合）

ＣＦＢモードの処理のみを行うときには、ＣＦＢモードの初期状態における処理が行われる。この場合は、図３の下段の処理Ｄ９及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック４は、暗号化データＣを入力とし、「Ｅｎｃｒｙｐｔ」処理を行って、データＩを求める。暗号モード共用処理ブロック４は、求められたデータＩと入力された初期ベクタデータＩＶデータとの排他的論理和を求めて、暗号化されていないデータＤとして出力する。

【００８８】

この場合の処理を、図２を参照して説明する。暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＦＢモードの初期状態であることを示す信号が入力される。

【００８９】

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、初期ベクタデータＩＶを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと初期ベクタデータＩＶとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

【００９０】

第３のセレクタ４３は、処理ブロック入力データＥＣを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

【００９１】

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データ

を用いて、第３のセレクタから出力された処理ブロック入力データＥＣに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして復号化結果を出力する。

【００９２】

６）５６ビット鍵モードであり、かつ、ＣＦＢモードの定常状態である場合（図４のＤＥＣ－ＣＦＢ　Ｎｏｒｍａｌの場合）

ＣＢＣモードの処理に続いてＣＦＢモードの処理を行うときには、ＣＦＢモードの定常状態における処理が行われる。この場合は、図３の下段の処理Ｄ９及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック４は、その前のＥＣＢ処理で用いた暗号化データＣを入力とし、「Ｅｎｃｒｙｐｔ」処理を行って、データＩを求める。暗号モード共用処理ブロック４は、求められたデータＩと次の暗号化データＣとの排他的論理和を求めて、暗号化されていないデータＤとして出力する。

【００９３】

この場合の処理を、図２を参照して説明する。暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＦＢモードの定常状態であることを示す信号が入力される。

【００９４】

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、処理ブロック入力データＥＣを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと処理ブロック入力データＥＣとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

【００９５】

第３のセレクタ４３は、遅延器４８が出力する遅延された処理ブロック入力データＥＣＤを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ

処理器４７に出力する。

【００９６】

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された遅延された処理ブロック入力データＥＣＤに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして復号化結果を出力する。

【００９７】

７）５６ビット鍵モードではなく、かつ、ＣＦＢモードの初期状態である場合

８）５６ビット鍵モードではなく、かつ、ＣＦＢモードの定常状態である場合

これらの場合は、それぞれ５），６）の場合と次の点を除いて同じである。すなわち、暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードではないことを示す信号が入力される。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードではないことを示す信号が入力されているので、入力された５６ビットの鍵データＫＤのうち、必要がないビット（例えば上位１６ビット）をマスクして、４０ビット鍵データとしてＥＣＢ処理器４７に出力する。ＥＣＢ処理器４７は、ビットマスク器４６から出力された４０ビット鍵データを用いてＥＣＢ処理を行う。

【００９８】

暗号モード共用処理ブロック４の暗号化処理時の動作について、図２、図３の上段、及び図４を参照して説明する。この場合、暗号モード共用処理ブロック４には、暗号化／復号化切り替え信号ＳＳとして、暗号化を示す信号が入力される。５６ビット鍵モードであるか否か、ＣＢＣモード及びＣＦＢモードのうちのいずれであるか、初期状態及び定常状態のうちのいずれであるかによって場合を分けて説明する。ＥＣＢ処理器４７におけるＥＣＢ処理は、ＣＢＣモードの場合及びＣＦＢモードの場合ともに暗号化処理である。

【００９９】

９）５６ビット鍵モードであり、かつ、ＣＢＣモードの初期状態である場合（図４のＥＮＣ－ＣＢＣ　Ｉｎｉｔの場合）

この場合は、図３の上段の処理Ｅ１及びその前の排他的論理和を求める処理が行われる。暗号モード共用処理ブロック４は、入力された初期ベクタデータＩＶと暗号化されていないデータＤとの排他的論理和を求めて、データＩとして出力する。暗号モード共用処理ブロック４は、得られたデータＩにＥＣＢ処理として「Ｅｎｃｒｙｐｔ」処理を行って、暗号化データＣを求めて出力する。

【０１００】

この場合の処理を、図２を参照して説明する。暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＢＣモードの初期状態であることを示す信号が入力される。

【０１０１】

第１のセレクタ４１は、処理ブロック入力データＥＣを選択して出力する。第２のセレクタ４２は、初期ベクタデータＩＶを選択して出力する。排他的論理和演算器４９は、処理ブロック入力データＥＣと初期ベクタデータＩＶとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

【０１０２】

第３のセレクタ４３は、排他的論理和データＥＲを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

【０１０３】

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された排他的論理和データＥＲに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、暗号処理データＰＤを選択して、処理済データＤＣとして暗号化結果を出力する。

【０１０４】

１０）５６ビット鍵モードであり、かつ、ＣＢＣモードの定常状態である場合（図４のＥＮＣ－ＣＢＣ　Ｎｏｒｍａｌの場合）

この場合は、図３の上段の処理Ｅ２又はＥ３及びこれらのそれぞれの前の排他的論理和を求める処理が行われる。暗号モード共用処理ブロック４は、暗号化されていないデータＤとその前のＥＣＢ処理で得られた暗号化データＣとの排他的論理和を求めて、データＩとして出力する。暗号モード共用処理ブロック４は、得られたデータＩにＥＣＢ処理として「Ｅｎｃｒｙｐｔ」処理を行って、暗号化データＣを求めて出力する。

【０１０５】

この場合の処理を、図２を参照して説明する。暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＢＣモードの定常状態であることを示す信号が入力される。

【０１０６】

第１のセレクタ４１は、処理ブロック入力データＥＣを選択して出力する。第２のセレクタ４２は、遅延器４８が出力する遅延された暗号処理データＰＤＤを選択して出力する。排他的論理和演算器４９は、処理ブロック入力データＥＣと遅延された暗号処理データＰＤＤとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

【０１０７】

第３のセレクタ４３は、排他的論理和データＥＲを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

【０１０８】

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された排他的論理和データＥＲに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、暗号処理データＰＤを選択して、処理済データＤＣとして暗号化結果を出力する。

【０１０９】

１１）５６ビット鍵モードではなく、かつ、ＣＢＣモードの初期状態である場

合

１２）５６ビット鍵モードではなく、かつ、ＣＢＣモードの定常状態である場合

これらの場合は、それぞれ９），１０）の場合と次の点を除いて同じである。すなわち、暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードではないことを示す信号が入力される。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードではないことを示す信号が入力されているので、入力された５６ビットの鍵データＫＤのうち、必要がないビット（例えば上位１６ビット）をマスクして、４０ビット鍵データとしてＥＣＢ処理器４７に出力する。ＥＣＢ処理器４７は、ビットマスク器４６から出力された４０ビット鍵データを用いてＥＣＢ処理を行う。

【０１１０】

１３）５６ビット鍵モードであり、かつ、ＣＦＢモードの初期状態である場合（図４のＥＮＣ－ＣＦＢ　Ｉｎｉｔの場合）

ＣＦＢモードの処理のみを行うときには、ＣＦＢモードの初期状態における処理が行われる。この場合は、図３の上段の処理Ｅ９及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック４は、暗号化されていないデータＤを入力とし、「Ｅｎｃｒｙｐｔ」処理を行う。暗号モード共用処理ブロック４は、この処理で求められたデータと入力された初期ベクタデータＩＶデータとの排他的論理和を求めて、暗号化データＣとして出力する。

【０１１１】

この場合の処理を、図２を参照して説明する。暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＦＢモードの初期状態であることを示す信号が入力される。

【０１１２】

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、初期ベクタデータＩＶを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと初期ベクタデータＩＶとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲ

を出力する。

【０１１３】

第３のセレクタ４３は、処理ブロック入力データＥＣを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

【０１１４】

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された処理ブロック入力データＥＣに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして暗号化結果を出力する。

【０１１５】

１４）５６ビット鍵モードであり、かつ、ＣＦＢモードの定常状態である場合（図４のＥＮＣ－ＣＦＢ　Ｎｏｒｍａｌの場合）

ＣＢＣモードの処理に続いてＣＦＢモードの処理を行うときには、ＣＦＢモードの定常状態における処理が行われる。この場合は、図３の上段の処理Ｅ９及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック４は、その前のＥＣＢ処理で得られた暗号化データＣを入力とし、「Ｅｎｃｒｙｐｔ」処理を行う。暗号モード共用処理ブロック４は、この処理で求められたデータと暗号化されていないデータＤとの排他的論理和を求めて、暗号化データＣとして出力する。

【０１１６】

この場合の処理を、図２を参照して説明する。暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＦＢモードの定常状態であることを示す信号が入力される。

【０１１７】

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、処理ブロック入力データＥＣを選択し

て出力する。排他的論理和演算器４９は、暗号処理データＰＤと処理ブロック入力データＥＣとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

【０１１８】

第３のセレクタ４３は、遅延器４８が出力する遅延された暗号処理データＰＤＤを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

【０１１９】

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された遅延された暗号処理データＰＤＤに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして暗号化結果を出力する。

【０１２０】

１５）５６ビット鍵モードではなく、かつ、ＣＦＢモードの初期状態である場合

１６）５６ビット鍵モードではなく、かつ、ＣＦＢモードの定常状態である場合

これらの場合は、それぞれ１３），１４）の場合と次の点を除いて同じである。すなわち、暗号モード共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードではないことを示す信号が入力される。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードではないことを示す信号が入力されているので、入力された５６ビットの鍵データＫＤのうち、必要がないビット（例えば上位１６ビット）をマスクして、４０ビット鍵データとしてＥＣＢ処理器４７に出力する。ＥＣＢ処理器４７は、ビットマスク器４６から出力された４０ビット鍵データを用いてＥＣＢ処理を行う。

【０１２１】

なお、モード選択信号ＭＳがＥＣＢモードを示す場合には、第３のセレクタ４３は処理ブロック入力データＥＣを選択して出力し、かつ、第４のセレクタ４４は暗号処理データＰＤを選択して出力する。ＥＣＢ処理器４７は、暗号化／復号化切り替え信号ＳＳが、暗号化を示す場合は暗号化処理を行い、復号化を示す場合は復号化処理を行う。すなわち、図１の暗号化復号化装置は、ＣＢＣモード及びＣＦＢモードに加えてＥＣＢモードにおける暗号化及び復号化を行うことができる。

【０１２２】

また、５６ビット鍵データ又は４０ビット鍵データに代えて、他の長さの鍵データを用いるようにすることも容易にできる。

【０１２３】

また、図１の暗号化復号化装置を暗号化装置として用いるようにしてもよい。この場合は、入力されたダウンストリームデータを暗号化して出力するのみでよく、以上の説明における復号化に対応した構成及び動作は不要である。また、暗号化／復号化切り替え信号ＳＳは不要であり、第１～第４のセレクタ及びＥＣＢ処理器は、モード選択信号ＭＳに従って動作すればよい。

【０１２４】

より具体的には、遅延器は、暗号処理データＰＤを入力とし、これを遅延させて出力する。第２のセレクタは、処理ブロック入力データＥＣ、初期ベクタデータＩＶ、及び遅延器が出力する遅延した暗号処理データＰＤＤのうちのいずれかを選択して出力する。第３のセレクタは、処理ブロック入力データＥＣ、排他的論理和演算器が出力する排他的論理和データＥＲ、及び遅延した暗号処理データＰＤＤのうちのいずれかを選択して出力する。第４のセレクタは、暗号処理データＰＤ及び排他的論理和データＥＲのうちのいずれかを選択して、暗号化結果として出力する。

【０１２５】

また、図１の暗号化復号化装置を復号化装置として用いるようにしてもよい。この場合は、入力されたアップストリームデータを復号化して出力するのみでよく、以上の説明における暗号化に対応した構成及び動作は不要である。このため

、暗号処理データＰＤを常に出力する第１のセレクタ、及び排他的論理和演算器が出力する排他的論理和データＥＲを常に出力する第４のセレクタは不要である。また、暗号化／復号化切り替え信号ＳＳは不要であり、第２及び第３のセレクタ及びＥＣＢ処理器は、モード選択信号ＭＳに従って動作すればよい。

【０１２６】

より具体的には、遅延器は、処理ブロック入力データＥＣを入力とし、これを遅延させて出力する。第２のセレクタは、処理ブロック入力データＥＣ、初期ベクタデータＩＶ、及び遅延器が出力する遅延した処理ブロック入力データＥＣＤのうちのいずれかを選択して出力する。第３のセレクタは、処理ブロック入力データＥＣ、及び遅延した処理ブロック入力データＥＣＤのうちのいずれかを選択して出力する。排他的論理和演算器は、暗号処理データＰＤと第２のセレクタの出力との排他的論理和を求めて、復号化結果として出力する。

【０１２７】

また、本発明は、ＣＰＵやＤＳＰ（digital signal processor）等のプロセッサを用いたソフトウェアによる処理を行うことによって実現することも可能である。

【０１２８】

以上のように、本発明に係る暗号化復号化装置によると、モード選択信号を変化させれば、ＥＣＢモード、ＣＢＣモード及びＣＦＢモードのうちのいずれかと、５６ビット鍵モード又は４０ビット鍵モードのいずれかとを組み合わせたいずれのモードにおいても、同一のハードウェアによって暗号化データに対する復号化を行い、暗号解読データを得ることができる。

【０１２９】

また、暗号化／復号化切り替え信号を変化させれば、いずれのモードにおいても、データの暗号化及び復号化のいずれをも、同一のハードウェアによって行うことができる。

【０１３０】

また、以上の暗号化／復号化をソフトウェアによって行う場合も、前記組み合わせのいずれのモードにおいても同一のソフトウェアによって暗号化及び復号化

を行うことができる。

【０１３１】

【発明の効果】

以上のように、本発明によると、同一のハードウェアによって多くのモードにおいて暗号化／復号化を行うことができるので、回路面積を削減してコストを抑えることができる。ソフトウェアによって実現する場合においても、プログラムの簡略化等を図ることができる。多くの機能を低コストで提供することができるので、コストパフォーマンスを高めることができる。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る暗号化復号化装置の構成を示すブロック図である。

【図２】

図１の暗号モード共用処理ブロックの構成の例を示すブロック図である。

【図３】

図１の暗号モード共用処理ブロックが行う処理の流れを示す説明図である。

【図４】

図１の暗号モード共用処理ブロックの第１～第４のセレクタが選択するデータの組み合わせを示す説明図である。

【符号の説明】

２　データ構造解析ブロック

４　暗号モード共用処理ブロック

６　データ制御ブロック

４１　第１のセレクタ

４２　第２のセレクタ

４３　第３のセレクタ

４４　第４のセレクタ

４６　ビットマスク器

４７　ＥＣＢ処理器

４８　遅延器

４９　排他的論理和演算器

ＳＤ　ダウンストリームデータ

ＳＵ　アップストリームデータ

ＴＫ　ＴＥＫ制御用データ

ＥＣ　処理ブロック入力データ

ＳＳ　暗号化／復号化切り替え信号

ＭＳ　モード選択信号

ＩＶ　初期ベクタデータ

ＫＤ　鍵データ

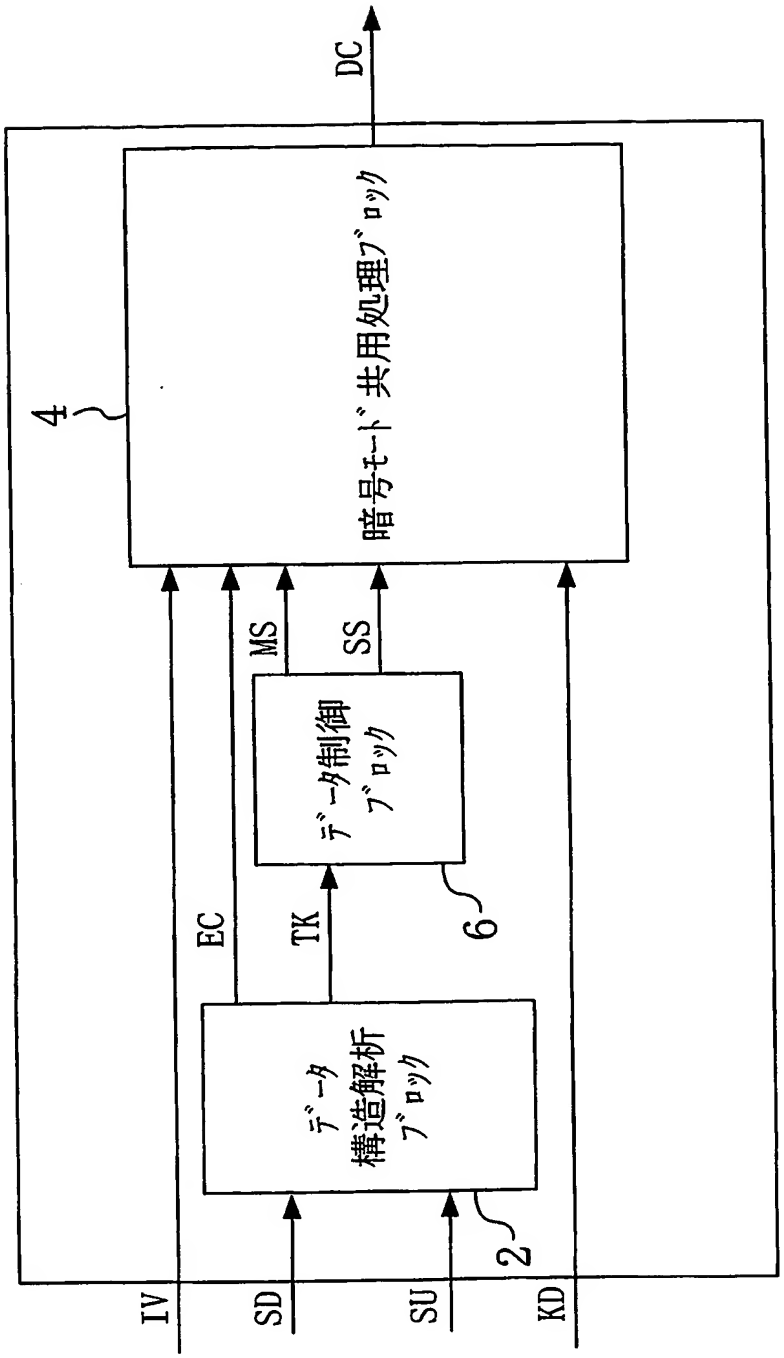
ＰＤ　暗号処理データ

ＥＣＤ　遅延した処理ブロック入力データ

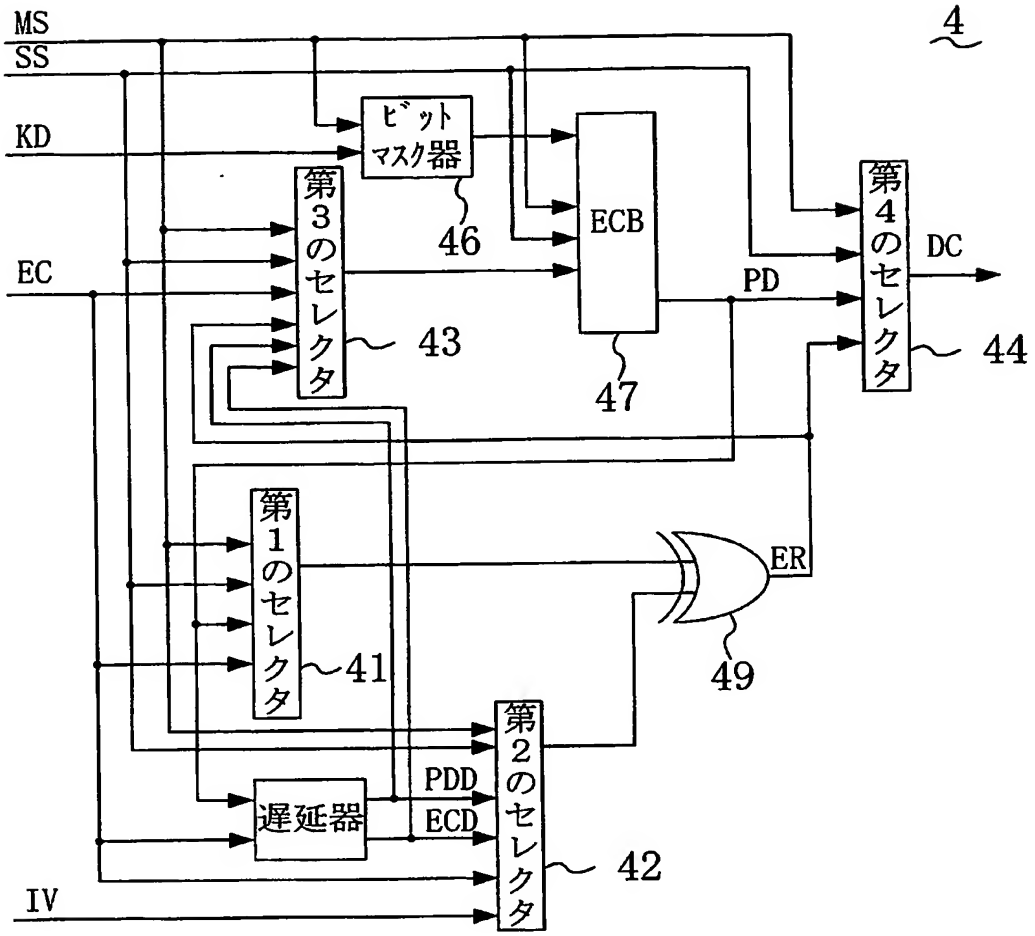
ＰＤＤ　遅延した暗号処理データ

【書類名】　図面

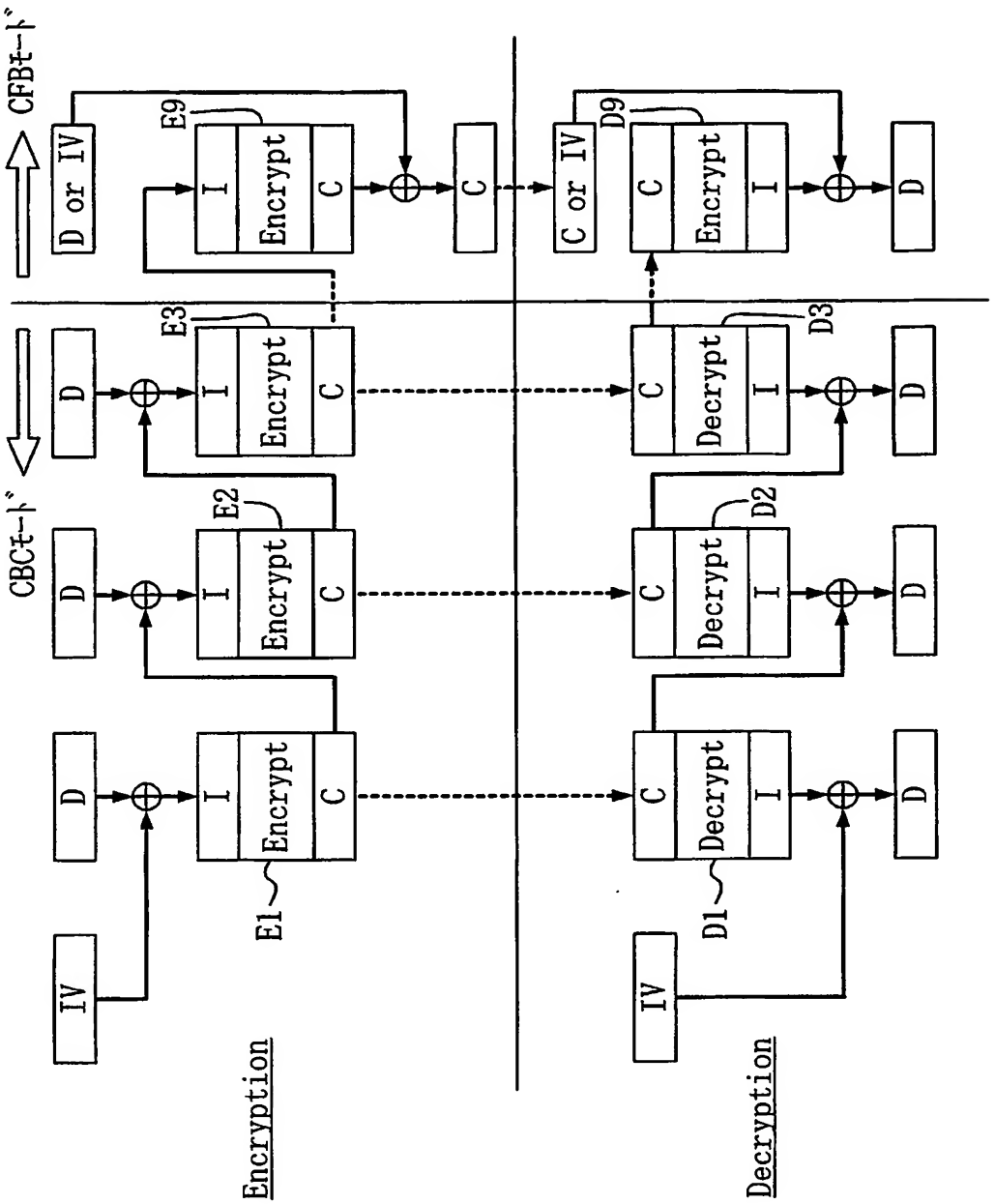
【図１】


DC
4
暗号ﾓｰﾄﾞ共用処理ﾌﾞﾛｯｸ
MS
SS
ﾃﾞｰﾀ制御
ﾌﾞﾛｯｸ
6
EC
TK
ﾃﾞｰﾀ
構造解析
ﾌﾞﾛｯｸ
2
IV
SD
SU
KD

【図２】


4
MS
SS
KD
EC
ビット
マスク器
46
第3のセレクタ
43
ECB
47
PD
第4のセレクタ
DC
44
第1のセレクタ
41
ER
49
第2のセレクタ
42
遅延器
PDD
ECD
IV

【図３】


CFBモード
CBCモード
D or IV
C or IV
E9
D9
E3
D3
E2
D2
E1
D1
I
Encrypt
C
Decrypt
D
IV
Encryption
Decryption

【図４】

	DEC-CBC Init	DEC-CBC Normal	DEC-CFB Init	DEC-CFB Normal	ENC-CBC Init	ENC-CBC Normal	ENC-CFB Init	ENC-CFB Normal
第1のセレクタ	PD	PD	PD	PD	EC	EC	PD	PD
第2のセレクタ	IV	ECD	IV	EC	IV	PDD	IV	EC
第3のセレクタ	EC	EC	EC	ECD	ER	ER	EC	PDD
第4のセレクタ	ER	ER	ER	ER	PD	PD	ER	ER

【書類名】　要約書

【要約】

【課題】　複数のモードで処理回路を共用化して、回路規模を削減する。

【解決手段】　暗号化復号化装置として、暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータを受け取り、ＴＥＫ制御用データ、及び、暗号化データ又は暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、ＴＥＫ制御用データに従ってモード選択信号を求めて出力するデータ制御ブロックと、処理ブロック入力データに対して暗号化又は復号化を行い、得られた結果を出力する暗号モード共用処理ブロックとを備える。暗号モード共用処理ブロックは、入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、モード選択信号に示されたモードで暗号化又は復号化を行う。

【選択図】　図１

特願２００２－２３１２８４

出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.